プリンターの新領域をひらく

SECURITY POLICY

セキュリティ ポリシー

■ はじめに

理想科学では、プリンター製品のご提供にあたり、お客様の貴重な情報資産を漏洩リスクから守り、安心して製品をご利用いただけるよう、積極的な取り組みを行なっています。

ただし、ネットワークに接続してご利用いただく製品の場合、ご使用方法によっては情報漏洩リスクが高まる場合があります。
本書をお読みいただき、適切な設定でご使用いただけますようお願い申し上げます。

万一、新たなセキュリティの脅威が発生した場合にも、理想科学は速やかな対策が取れる体制をとっております。引き続き安心してご利用いただきますようお願いいたします。

■ 当社製品のセキュリティ対応体制

理想科学はセキュリティ対策を製品に反映する、さまざまな体制を整えています。

製品の動作プログラムリリース時に第三者による脆弱性チェック

動作プログラムの脆弱性は、自社検証に加え専門企業による第三者チェックを受けた後リリースしています。

リリース後も脆弱性チェックを実施し適切な対応

製品のリリース後も継続してプログラムの脆弱性チェックを行い、新規の脆弱性に対応しています。

保守サービス網を利用したプログラムの更新

保守サービス網を利用し、お客様がお使いの製品への対策についても迅速に展開を行っています。

※ リリース後もチェックを実施

■ ネットワーク接続について

ネットワークに接続可能な機器は、外部からのアクセスおよび情報漏洩のリスクがあります。
以下をご留意いただくことでリスクを低減できます。

不要なポートをあけない

待ち受けポートがあると、外部からの侵入の恐れがあります。不要なポートは閉じてください（製品の初期設定では機能上、必要なポート以外は閉じています）。さらにこのページに記載された機能を使用することで、不正なアクセスや操作ができなくなり、侵入リスクを低減できます。

アクセスできるパソコンを指定

接続可能な送信元IPアドレスを制限することで、許可していないIPアドレスからの接続を制限することができます。

ログイン認証が必要な運用

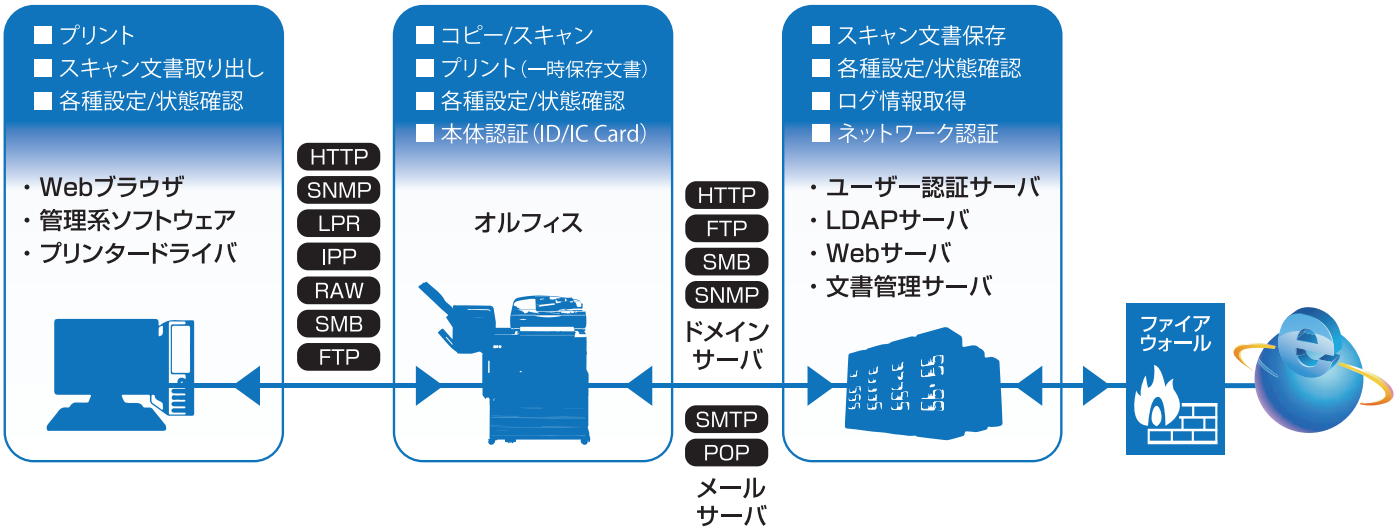
使用時にログイン認証を必要とすることで、製品を使用するユーザーを制限することができます。

通信の暗号化

コンソールの通信をhttpsプロトコルに設定できます。

ネットワーク接続イメージ

※図はオルフィスシリーズの例です。



USBメモリの接続について

●理想科学の製品は、USBメモリを認識しても自動実行を行わないため、ウイルス感染の心配はありません。また、パソコンのUSB接続機器のように様々なデバイスドライバがインストールされることはありません。
●製品にキーボードやマウスを接続することができたとしても、コマンドが使える状態にはなりません。
●USBメモリ接続には、ハッカーによるクラッキングのほか、不適切な運用をした場合はプリンター本体内の蓄積データの漏洩リスクがあります。
●プリンター本体内にはUSBメモリから取り込んだ機密文書を残さないようにしてください。残す場合には必ずパスワードを設定してください。

※一部リソグラフにはない機能があります。

データ送信について

スキャンした画像データのFTP・SMB・SMTP送信が可能なため、これらプロトコルを使用するネットワーク機器と同等の配慮が望まれます。
また、スキャンした画像データはプリンター本体HDDに蓄積できますが、本体内には機密文書をできるだけ残さず、残す場合には必ずパスワードを設定してください。

※一部リソグラフにはない機能があります。

プリントジョブについて

ボックスに出力したプリントジョブは本体HDDに保存され、運用によっては漏洩リスクが高まります。
プリンター本体内には機密文書をできるだけ残さず、残す場合には必ずパスワードを設定してください。

※一部リソグラフにはない機能があります。

管理者パスワード設定について

正しい運用を継続するには管理者による適切な環境および設定管理が必要です。管理者権限を持つユーザーには必ずログインパスワードを付与してください。
管理者権限を持つユーザーでログインした場合、本体蓄積データの操作・設定の変更が可能となります。

●詳しい操作方法は取扱説明書をご覧ください。●記載の内容は2015年10月現在のものです。

資料請求・お問い合わせ
お客様相談室 0120-534-881
受付時間 10:00～12:00 13:00～17:00（土・日・祝日・夏期休業・年末年始を除く）
ホームページ http://www.riso.co.jp/

理想科学工業株式会社 本社/〒108-8385 東京都港区芝5-34-7 田町センタービル